Internet of things Security Implementation using Blockchain for Wireless Technology

Karim Jabur Karim

A project report submitted in partial
Fulfillment of the requirement for the award of the
Master of Electrical Engineering with Honours

Faculty of Electrical and Electronic Engineering
Universiti Tun Hussein Onn Malaysia

JULY 2019

ACKNOWLEDGEMENT

Praise and thanks be to **Allah** for the blessings of mind and health and "conciliating me" for completing this thesis. I would like to express my sincere gratitude to my supervisor **Dr. Nan bin Md Sahar** for giving me the proper of advice, guidance and encouragement for my research. He gave me many opinions and ideas for the research and writing of this thesis. Through his patience, motivation, enthusiasm and immense knowledge, I managed to complete this project perfectly and successfully!

In addition, I would like to thank my parents **JABUR** and **SAFANAH** for giving me ethical support while I were doing this project. They always guided me to make sure I could finish my project on time and complete it successfully.

To my wife **SAHAR**: Thank you for believing in me, and for your patience during so many days and nights! Thank you for all the things which you you have no idea what you've for me To my brothers and sisters. To my kids: You are always happy with every success that I do thanks a lot for your ethical support

To **UTHM** and the Faculty of Electrical and Electronic Engineering staff: Thanks for providing me with an excellent research environment and the proper resources to undertake this research. To the Iraqi government and all Universities: Thank you for supporting me to complete my master's degree. Last but not least, I would like to thank a person who contributed to completing my final thesis directly or indirectly. I would like to acknowledge him/her for helping, which was necessary to complete this.

Furthermore, I also would like to thank **my friends** for their concern and help for completing my project successfully with giving suggestions and discussing together to solve the problem during my project; without them, I could not have completed this project on time

ABSTRACT

Blockchain is a new security system which group many data into a block or so called classifying the data into a block. The block can have many types and each of them content data and security code. By using a decentralize mechanism, one security code protect all the data. That could happen at the server. In this research, a network of wireless sensor technology is proposed. The transmission of sensor data is via the Internet of things (Internet of Thing) technology. As many data transmitted, they have to classified and group them into a block. All the blocks are then send to the central processing unit, like a microcontroller. The block of data is then processed, identified and encrypted before send over the internet network. At the receiver, a GUI or Apps is developed to open and view the data. The Apps or GUI have an encrypted data or security code. User must key in the password before they can view the data. The password used by the end user at the Apps or GUI must be equivalent to the one encrypted at the sensor nodes. This is to satisfy the decentralized concept used in the Blockchain. To demonstrate the Blockchain technology applied to the wireless sensor network, a MATLAB Simulink function is used. The expected results should show a number of block of data in cryptography manner and chain together. The two set of data. Both have the data encrypted using hash. The black dots indicate the data has been encrypted whereas the white dot indicate indicates the data is not encrypted. The half white and half black indicates the data is in progress of encrypted. All this data should arrange in cryptography order and chain together in a vertical line. A protocol called block and chain group the data into the block and then chain then. The data appears in the blocks and send over the network. As seen in the simulation results, the yellow color represents the user data. This data has a default amplitude as 1 or 5. The data is chained and blocked to produce the Blockchain waveform

Keywords: Blockchain, Internet of things, Wireless Sensor Network and MATLAB Simulink

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

CHAPTER 1

INTRODUCTION

1.1 Background of Study

Internet of things nowadays becoming more and more popular in sensor data communications. The system form a duplex communications where the transceivers are sending and receiving data via an internet network. The data from the sensors are processed by the controller, it is then depends on the controller to route the data into the network. By theory, if the network is complex, the controller always determine the shortest path and find out the shortest time to send the sensor data into the network. The data is then stored in the network. If user wants to receive the data, he or she must has a platform to download the data.

Sending the sensor data via an internet network, especially for Wireless Sensor Network always attacks by malicious. The Malicious is an internet hacker. It usually sending a harmful packet to attack the data. The data under attack may face the consequences of data lost or information have done stolen.

Because the existing of malicious, the security becomes vital in wireless sensor network system. The security must be strong enough to avoid data being stolen or lost in the network. In this project, a new era of security system called, 'Blockchain' has been proposed to secure the wireless sensor network data communication systems. The Blockchain is a technology developed by Bitcoin in year 2010 [1].

The general idea behind the Blockchain security system are the list of records (called blocks) that linked by system called cryptography. Every block contents a 'hash' and a 'hash' content information from the previous block.

The block is then propagate in the network and not realize on the center control of the node. This is to avoid failure of the network. To make the system more efficient on sending and receiving the data, the Blockchain uses 'decentralize' concept where peer to peer communication takes over the advantage of centralize communication system. By using decentralize communication system, data have done secured and less vulnerable by the system failure in the network [2].

The data is then called by the Apps at the user terminal. The data only able to present or display when the GUI (Graphical User Interface) is available in the user terminals.

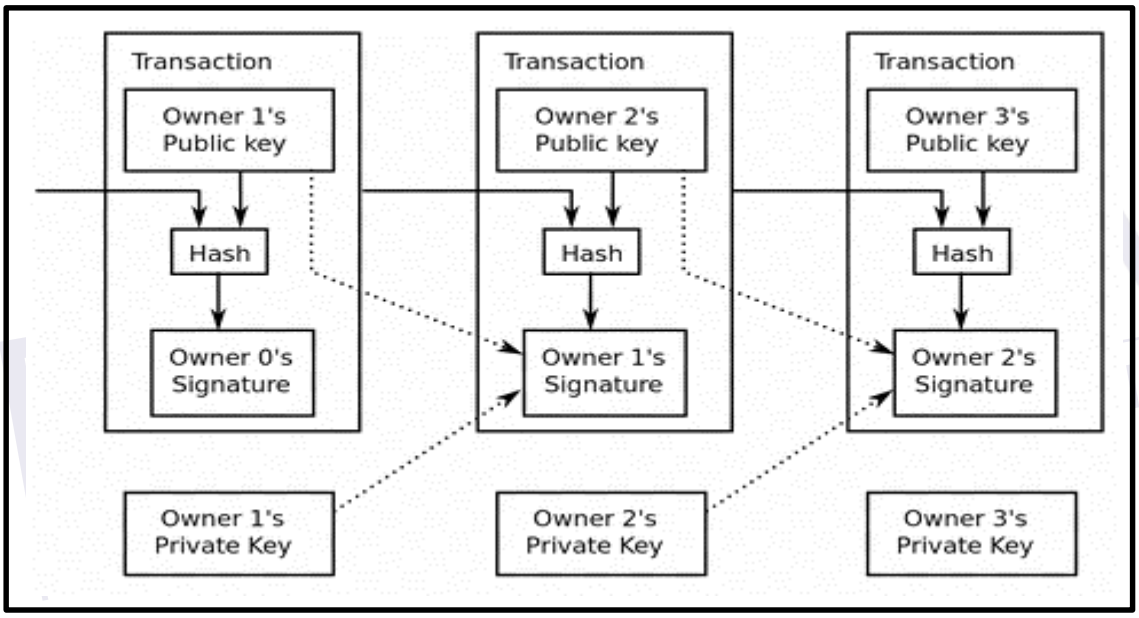

Figure 1.1: The concept of Blockchain and cryptography hash system [3]

To be more understand on how the Blockchain works, lets look at the secure monetary transaction system using Blockchain technology as shown in Figure 1.1.From Figure 1.1, assume that there are three transactions (three blocks). Each transaction is linked to each other, which means that they are correlated. Note that the first transaction on the most left carries information of owner 1, whereas the second transaction carries information on owner 2 and the last or third transaction on the right most carries information of owner 3.

When the first block or first transaction is just started, there is no previous transaction owner. Hence it is marked with '0 owner signature'. When the owner 1 makes transaction, his or her information have done deliver to second transaction. Note

that, this transaction information for owner 1 is intangible by owner 2. In other words, owner 2 not know there is an information of owner 1 content in his or her transaction. The owner 1 transaction information is stored in the database of the computer.

Similarly, when owner 2 makes transaction, his information have done appeared in the owner 3 transaction. And the owner 3 not know the transaction of owner 2. The information of owner 2 is intangible to the owner 3.

The process are then continues if more transactions (more blocks) are happen at the subsequence of time. More transactions create more blocks and hence form a main chain that linked together. The characteristics of each block (each transaction) are [4]

- The information content cannot be changed if the transaction is confirmed
- There is no way to alter the information as the information already locked
- User password is the first key to secure the transactions.

Now the question is, what is the advantage of putting all users' information from one block to another block? Does it secure?

The answer for the question above is 'yes', it is secure. Putting all the users' information from one block to another block can save the data search time and at the same time if one block of data is loss, the rest still contents the information. Thus, this help to backup the data as it propagates in the network. The security part of this is the main concern in this research and it have done applied into wireless sensor network Internet of things technology.

To use the Blockchain technology in wireless sensor network system, the algorithm proposed is shown below:

- Each block represents one sensor and every sensor has its own data to send
- When data of one sensor is obtained, the data have done appended to another sensor data
- Repeat step 2 to form a block of chain
- All the blocks are then compiled and send to the Internet of things network via a controller.
- User at the communication terminal can download the data via the Apps or GUI. The webpage is the GUI that can help to view the data.

Transforming the diagram shown in Figure 1.1 into the block that can applied into wireless sensor network is shown below:

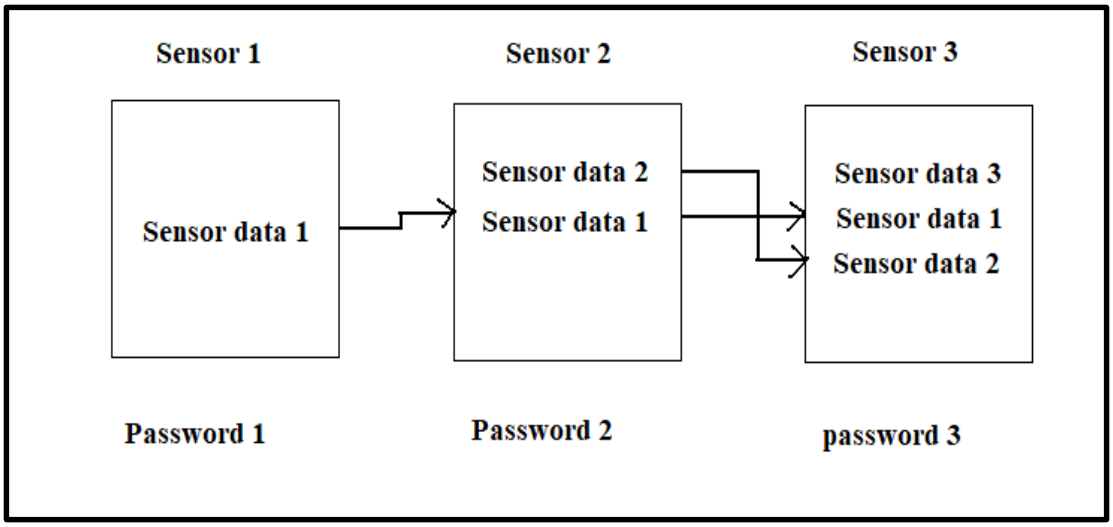

Figure 1.2: Blockchain equivalent security system applied in wireless sensor network [5]

All the blocks information are processed and saved into a databased. The processing of information is carried out by a microcontroller (an access node to all the sensors). The microcontroller then sends all the data into Internet of things network via a WiFi module. The scenario of the Blockchain-Internet of things system should be look like below:

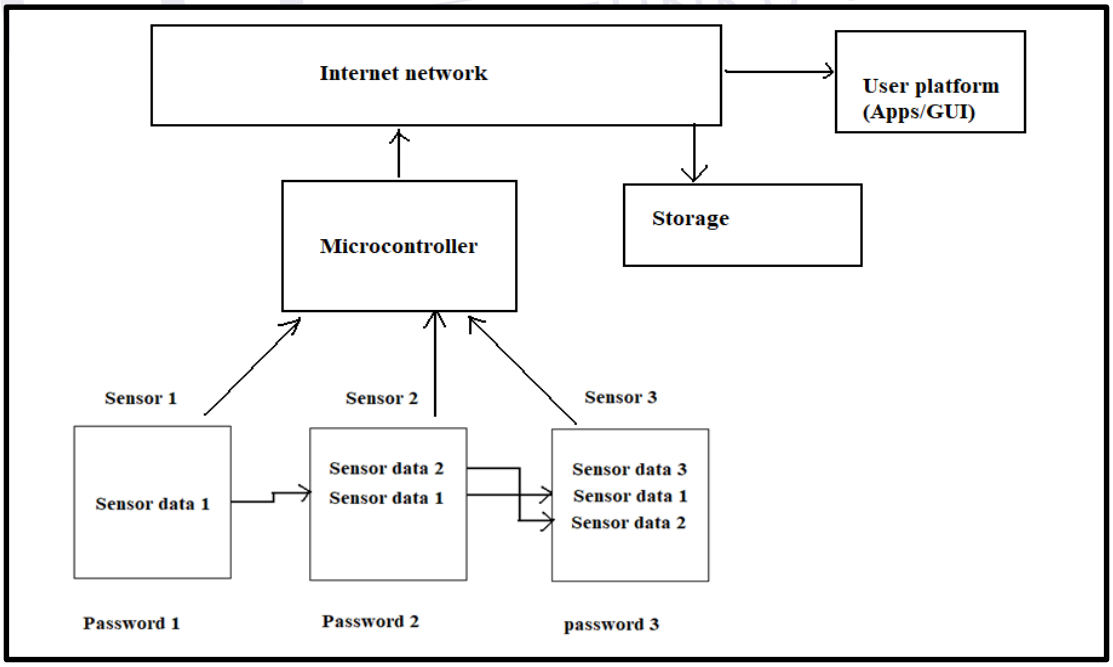

Figure 1.3: The Blockchain-Internet of things security system [6]

Note that, practically each sensor has its own processor or control unit. The sensor connect to microcontroller is via wireless technology. Typical frequency used

is 2.4 GHz, which is under WiFi category. Since the proposed idea of this research is a software based, so a modelling of Figure 1.3 have done applied to study the protocol of Blockchain in security system. For convenient to demo and present of Blockchain-Internet of things security base system, a MATLAB Simulink block function is employed. MATLAB is a powerful tool. Its Simulink function consists of many libraries that can support to build up the Blockchain.

The simulation of Blockchain modelling of Internet of things should produces the following results

- The GUI to show each block that contain information of previous block (Basic Blockchain rules applied)
- The GUI to show the sensor data to be protected by password (Basic security system in Blockchain)
- The GUI to view the data that send from the sensors
- The algorithm of Blockchain.

The final outcome of the research should be an animation of program to show the basic Blockchain-Internet of things security system applied in wireless sensor network.

1.2 Problem Statement

Blockchain is a technology used to secure the transaction. But sadly to say that this technology only applied in monetary transaction. Until now its strength still ambiguous to the engineering applications [21].

The main concern of the Blockchain is not the 'block' itself only, but the security system. For current wireless sensor network technology, there is no security add on. If there is, just a simple security for the entire system. A simple security for entire system means, one key of password to protect all the system. This could be dangerous. If the key lost, then the whole system is in 'lock' condition.

For Blockchain security, it has the advantage that if one block of data missing, the data still can retrieve back because multiple information is duplicated in other blocks.

Protecting the sensor data sometimes are needed. This is because some of the sensor data are confidential and they might information used for other researches. So it is not surprising that people nowadays wanted to protect the sensor data [22].

Where the statistic presents the total number of Blockchain wallet users worldwide, from the first quarter of 2015 to third quarter of 2018. The number of Blockchain wallets has been growing since the creation of the Bitcoin virtual currency in 2009, reaching over 28 million Blockchain wallet users at the end of September 2018 shown in Figure (1.4)

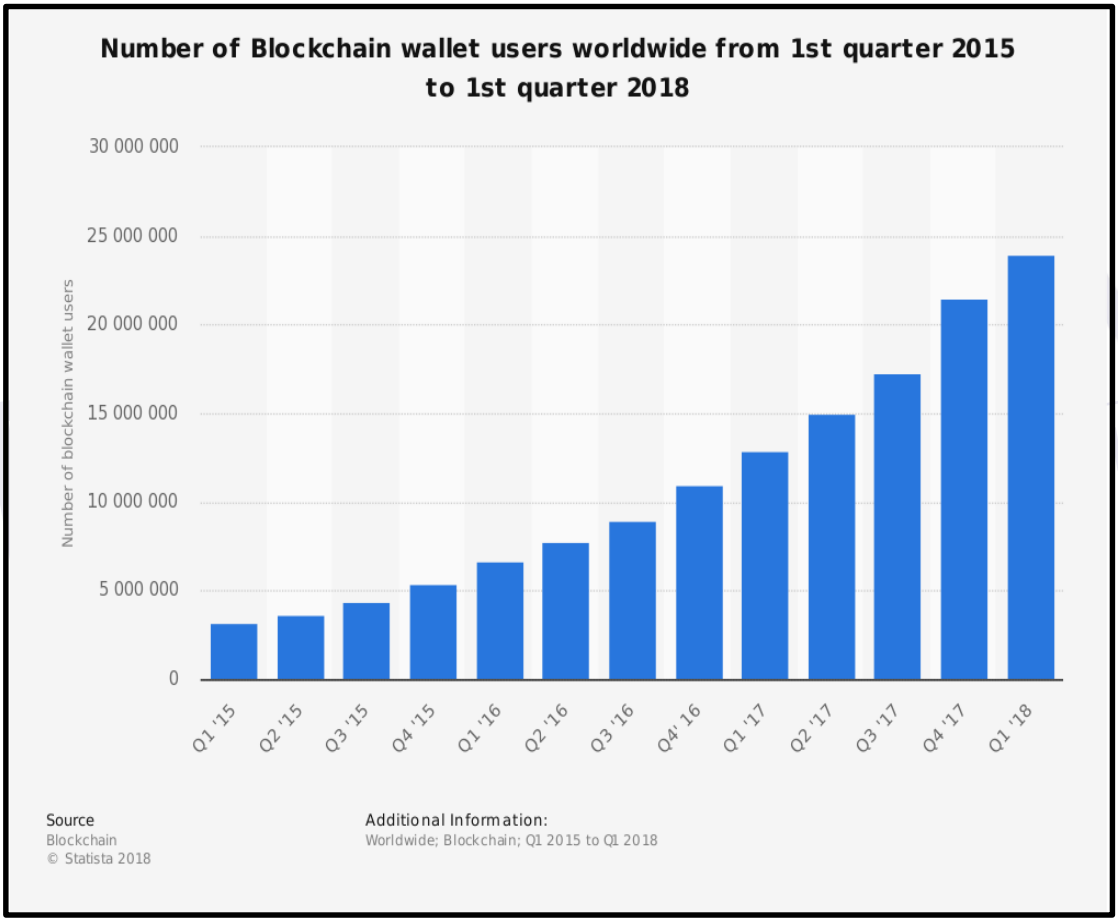

Figure 1.4: Number of Blockchain wallet users worldwide from 1st quarter 2015 to 3rd quarter 2018

1.3 Objectives of the Study

The research objectives are.

1. To Design and model the Internet of things system using MATLAB Simulink
2. To do simulation the outcomes of the Internet of things system.
3. To evaluate security performance in the blockchain algorithm in term of Detection? Blocking attack.

1.4 Scope of Project

Since the research keywords are Internet of things and Blockchain there are several research topics have to focus in order to meet the objectives. These research topics are:

- The Blockchain algorithm design and the application of this technology in wireless sensor network
- Evaluate security performance in the blockchain algorithm
- Use the MATLAB coding and Simulink to show the result.

The main idea of this research is to understand the Blockchain security system and the algorithm used.

Blockchain can be understood if many resources are available and most importantly, the correct resources must be available.

The limits of this project are limited to the use of the blockchain algorithm and the MATLAB environment. This algorithm is applied in the wireless network sensor this network is internal, not external, a proposal that can be developed to include the web in general.

Once the Blockchain theories are available and deeply understand how it works, the design works begin. The design works have done take the security system in the Blockchain and apply it into wireless sensor network. Certain things in Blockchain like transaction, means nothing to the engineering field, therefore anything related to the transaction by means of money have done be ignored in the research. On the other hand, anything related to the data protection, avoid malicious attack and data lost have done be applied to the wireless sensor network.

It is also important to review and study the MATLAB functions that suit to model the Internet of things using Blockchain security.

It take long time to learn the MATLAB compare to other works in the research. Therefore, more credit hour have done used to learn the MATLAB. Understanding the MATLAB operations and its library content are the basic things should have before model a wireless sensor network and apply the Blockchain algorithm. MATLAB modeling on Internet of things and apply the Blockchain have done challenge in this research.

Another focus area have done in the output of modeling. Running simulation not just to show the research or theories are working, but most importantly must understand the results produced by the simulation.

Step by step analysis of the results after simulation have done performed to know the entire operation of the Internet of things with Blockchain technology. Analysis have done carried out using brief explanation or using mathematical equations

1.5 Research Questions

To start up the research, there are always many questions appear. These questions should highlight at here. The answers for the questions have done shown after the research.

The research questions appear in this research are:

- How to model the Internet of things using MATLAB Simulink?
- How to apply Blockchain into MATLAB Simulink?
- Can the algorithm of Blockchain security system added into Simulink model?
- What are the outcomes should present after simulation?
- Is the animation enough to show the entire research?
- How to verify the outcome of the research is correct?
- How to get a free copy of MATLAB and have complete library of Simulink?

1.6 Report Arrangement

Generally, this report contents 5 chapters in total. The first chapter is introduction, second chapter is literature review, third chapter is methodology, fourth chapter is results and discussion and the final chapter is conclusion as well as recommendations.

Chapter one reviews the concept of Blockchain, security system and the Internet of things network implementation. The chapter also presents the research objectives, problem statements and the areas of the researches to be focused.

Chapter two shows the theories of Blockchain security and Internet of things in detail. This chapter also reviews some of the paper published and related to the Internet of things wireless sensor network. The most important things should exhibit in this chapter are the Blockchain theory, security and proved of published papers to show there is a Blockchain technology applied into wireless sensor network Internet of things system.

Chapter three presents step by step works on the modeling and design of the Internet of things. The chapter also show the algorithm of Blockchain with security. The complete flow chart present in this chapter to show the operation of the Blockchain in Internet of things system. The chapter also explain how to use the MATLAB to model the Internet of things and Blockchain system.

Chapter four shows the results and discussion. The results presented in this chapter are the simulation results. The animation results have done presented in this chapter to show the basic Blockchain operating system in Internet of things. Analysis of data lost and advantage of Blockchain security system also have done explained and presented in this chapter.

Chapter five is the conclusion and recommendation. This chapter concludes overall works of the research and presents some ideas to improve the research. The ideas presented to improve the research is considered a future works

CHAPTER 2

LITERATURE REVIEW

2.1 Introduction

This chapter presents the reviews of theories and principles of wireless sensor network security. The chapter also show the journal and conference papers that had published and related to the research. The important of papers have done guide the research to get some ideas and benchmarks on the direction of research. The papers also help to find out the research gaps and latest technology used in the wireless sensor network security system.

The chapter have done to show the theory about the blockchain and then moves on to discuss about the security system in wireless sensor networks. The key technologies and ideas have done highlighted at the end of the chapter.

2.2 Blockchain Technology

The founder of Blockchain technology was Bitcoin [7]. This technology was suggested since 2010 [7], but not widely used. Until late in year 2013 and 2014, Bitcoin getting more and more popular in investment business, then Blockchain becoming more and more important.

The purpose of developing the Blockchain is to secure the transaction in security system. This is the first thing, which the Blockchain must promise. According to Bitcoin, the Blockchain makes the transaction much secure and this has been introduced to many local banks.

Before understanding how the Blockchain works, it is better to know the terms or keywords used in the Blockchain. Table 2.1 summarized the keywords or terms used in Blockchain technology.

Table 2.1: Terms and keywords used in Blockchain technology [8]

No.	Terms or keywords	Meaning
1	Decentralize	Spread the networks into several center and each center is connected. All the centers in the network have their own nodes connected
2	Center	Refers to center processing unit or gateway. This are usually servers or WiFi gateway
3	Nodes	User terminals such as computers or wireless communication devices
4	Hash	Content input information that placed in a secure way. The hash result is series of secret code, which human cannot understand. The hash output length and size are determined by the input's length and size
5	Cryptography	Putting the message or information in secure way. This is basically a kind of encryption in network security

The operation of the Blockchain begins from the user terminal. Let's take a money transaction as an example to understand the Blockchain.

Assuming a user wants to request a transaction. This request information is broadcast to the network within one center control. Other nodes connected in the same center and in the same network receive the requests as well. The network then verified the requests.

If the request of transaction is approved, a block created by the center. The center then released the block so that it can combine with other blocks from other networks to form a Blockchain. Once the blockchain is formed, it cannot be altered. This blockchain is a secure system that content user information within the decentralize network.

A notification of successful transaction have done send back to the sender who request the transaction. This is called acknowledgement message to notify user about successful transaction [9].

The general idea about the Blockchain technology used in money transaction can be seen in Figure 2.1.

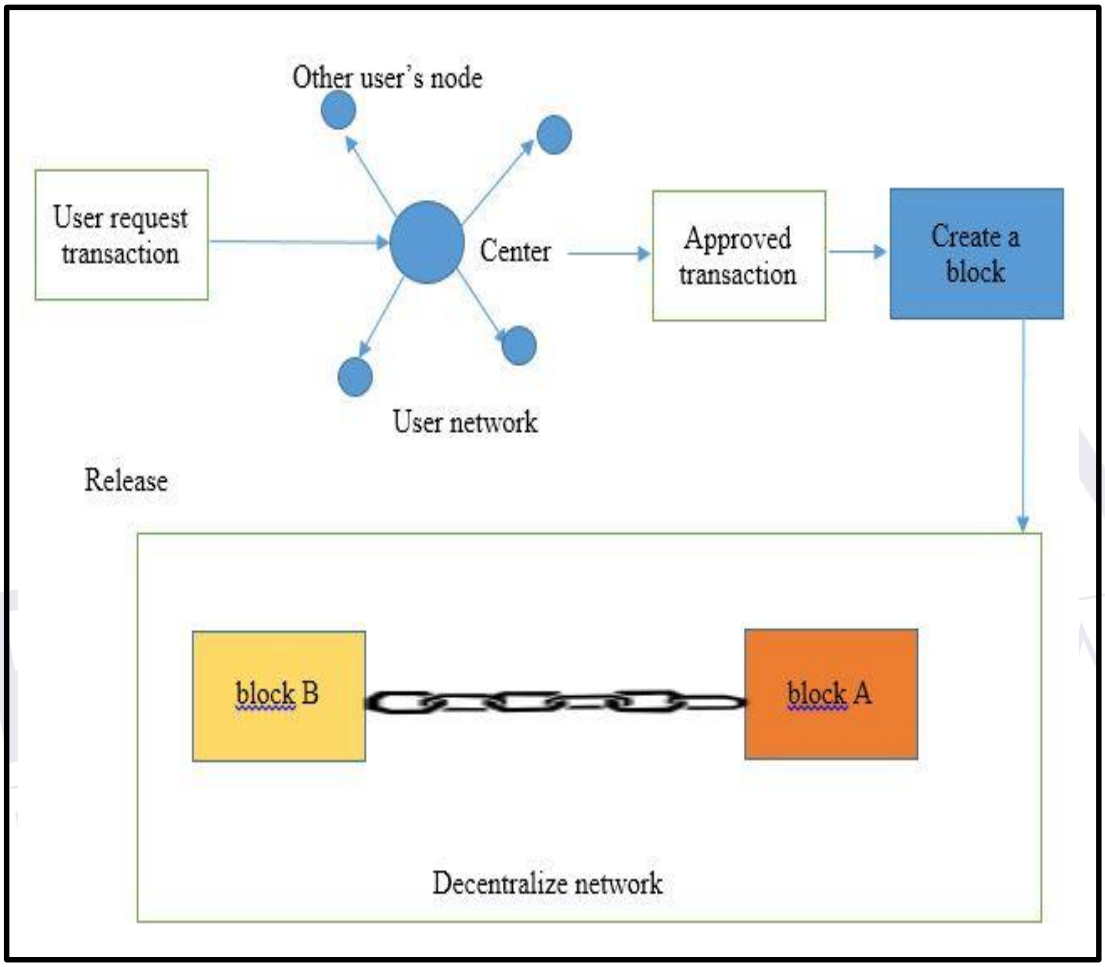

Figure 2.1: System Blockchain apply into transaction [10]

2.3 Sensor Data in Block Chain

Since the concept of block chain has been known, now we can apply block chain technology into the sensor data

Combining the blocks means combine all the data in the form of tightened series of data where it looks like a chain virtually. The chain consists of blocks of data

where each data is protected by its own password and username. The algorithm to create the block and chain to tighten the blocks is shown in Figure 2.3.

Initially, every sensor node process the data and save the data into a block. This block is protected by password. Every single sensor node has its own password. So, different sensor nodes have different password.

The sensor then send the data block to the center processing unit (the decentralize unit). In the center processing unit, the system combine all the data and put them in a group. The group basically is a chain that locked all the data related to that network. A name have done given to the group of data and once again, a password for that group of data is created.

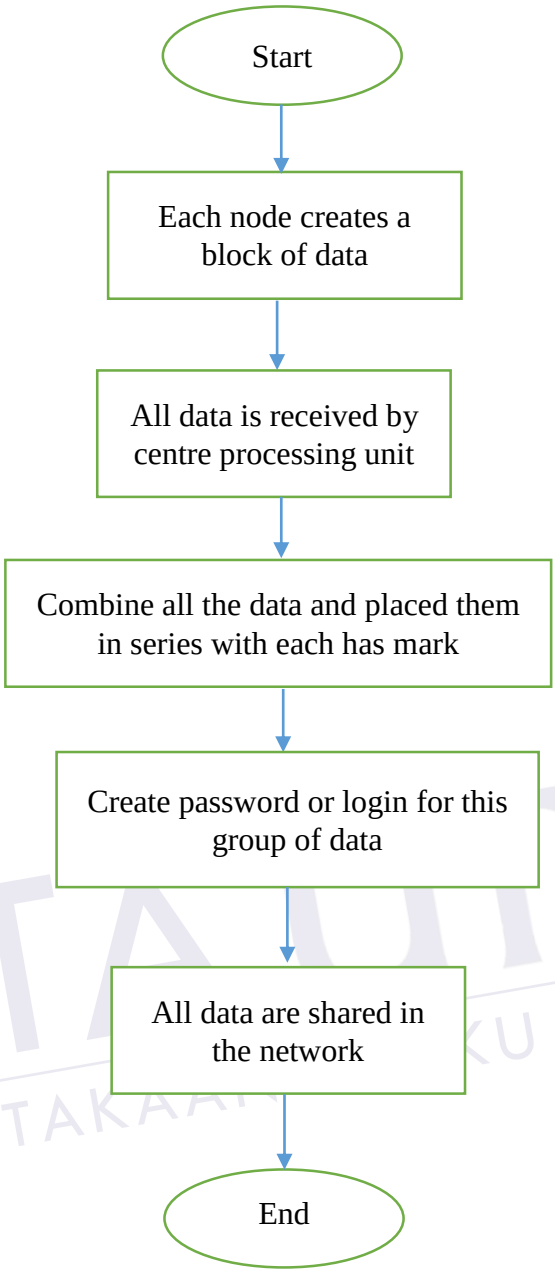

Figure 2.3: Block chain technology applied to wireless sensor Internet of things network [17]

Finally, the group of data is allow released into the network and just propagate around the network only. Therefore, whoever belongs to this network can access and grab the data. To retrieve the data, the user must know the password.

From the system wireless sensor data network, it can be seen that there are two protections of data. One is at the sensor node and the other one is at the center processing unit.

To access the network, user has to login into the center processing unit first. This is the main server and controller. It acts like an administrator.

Once user login, the system list down all the sensor data ready to be viewed. Once user click or choose one particular sensor data wanted to be viewed, another request of password appear.

2.4 Internet of things Block Chain Parameters

To be able model the Internet of things network with block chain technology, it is important to know some of the inputs and output parameters. These output parameters are used determine the performance of the networks and perform the judgment on the quality control.

The parameters of the block chain Internet of things system consists of two types: input parameters and output parameters. Table 2.1 shows the parameters and their meaning.

Table 2.2: Param8eters of Internet of things network [18]

Input parameters	**Meaning**	**Output parameters**	**Meaning**
Number of nodes	Number of sensor nodes in Internet of things	Total packets received by the center processing unit	Determine total data received by center processing unit
Queue length	To determine access time into the network	Total packet send	Determine total packet send in byte
Network area	Scale the network size	Average end to end delay	Compute the delay of communication
Initial energy	Overall power usage of the nodes	[redacted]	
Packet size	Determine the data size like in kb or Mb		
Malicious attack	Bad packet or data		

The input parameters are important for simulation purposes. The input parameters basically are used to setup or configure the network. When these parameters are changed, it affect the whole performance of the system.

The output parameters are the final outcomes that need to be observed after simulation. The output response when input is adjusted. The output parameters are appear in the form of values or waveform. Depending on what need to be observed in the overall network.

2.5 The Practical Internet of things Network

The practical Internet of things network comprises of sensor nodes, client or server and some protocol that govern the operation of the system. A simple Internet of things network can be seen in Figure 2.4.

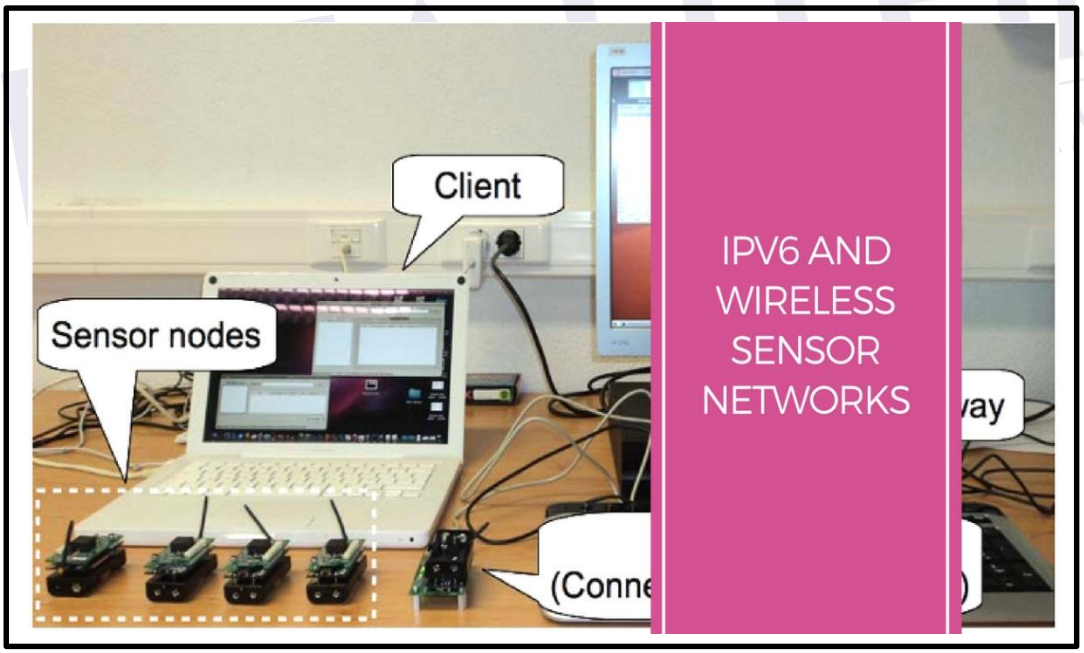

Figure 2.4: The practical Internet of things network [19]

Most of the practical Internet of things network using wireless sensor nodes to send the data to the client. The data does not need to protect because these data is not a sensitive data. They are the data of temperature, humidity, light intensity and object detection. All these data is less than 100 kB of size.

REFERENCES

1 Zibin Zheng, Hong-Ning Dai and Shaoan Xie, "An Overview of Blockchain Technology:Architecture, Consensus, and Future Trends", IEEE International Congress on Big Data, Vol.23, No. 10, 2017.

2 Carmen Holotescu, "Understanding Blockchain Technology and How to get Involved", IEEETrans on Big Data, Vol. 33, No. 12, pp. 89 – 100, 2016.

3 Michael Crosby, Nachiappan and Pradhan Pattanayak, "Blockchain Technology Beyond theBitcoin", Sutardja Centre for Entrepreneurship & Technology Technical Research, October16, 2015.

4 Khudnev and Evgenii, "Blockchain: Foundational Technology to Change the World", ResearchThesis, 2017.

5 Yongjun Ren, Yepeng Liu, Sai Ji and Arun Kumar, "Incentive Mechanism of Data StorageBased on Blockchain for Wireless Sensor Networks", Research Article Mobile InformationSystems, Vol. 2018.

6 Tiago M and Paula Fraga, "A Review on the Use of Blockchain for the Internet of Things",IEEE Access for Big Data, Vol. 10, 2018.

7 Lee Seng Yi and Kuang Qiao Ling, "Introduction to Blockchain Technology", IEEE Trans onComputing Technology, Vol. 10, Issue 1, pp. 4 – 20, 2015.

8 Janet.T, K.K.Devi, S. Kumaran, "The Block Chain Technology and Security Implementationin Computer Network", International Journal on Communications, Vol. 13, Issue 3, pp. 3 –12, 2015.

9 Suang.K, Rozila.M and Ali.H, "Important of Security System Using Blockchain Technology",International Journal on Engineering Technology, Vol. 23, Issue 17, pp. 5 – 15, 2016.

10 Mumitong.J, Riza.K and George.T, "Enhance Security Using Blockchain", IEEE Trans onEngineering and Security of Data, Vol. 90, Issue 24, pp. 16 – 25, 2017.

11 Norazlina.M and Nasrin.S, "Design and Implementation of Blockchain Security Coding" International Journal on Computer Sciences, Vol. 44, Issue 21, pp. 13 – 28, 2017.

12 Lucas. H and Dr. Hu, Introduction to Modern Data Communication with Security Enhancement, McGraw-Hill, New York, 2016.

13 Kau San and Liew Hai, Data Communication and Security, Prentice-Hall, New York, 2015.

14 Shella. J, Fundamental of Modern Data Communication and Protections, Oxford Press London, 2016.

15 Fanci. H and Lee Ping, Modern Data Communications and Protections, Pearson, New York,2016.

16 Voon.K, Natasha.Y and Chen. J, "The Blockchain Security Algorithm Design", IEEE Trans on Data Communications, Vol. 43, Issue 32, pp. 30 – 45, 2017.

17 Daslop. H and Jaisalu. E, "Blockchain Technology for Wireless Sensor Network", IEEE Trans on Electronic Communications, Vol. 67, Issue 41, pp. 36 – 69, 2017.

18 Ling Foon, Introduction to Blockchain Technology and Analysis, Longman, New York, 2016.

19 Tan Fung Pin and Hao Jie, "Practical Wireless Sensor Network and Internet of things", IEEE Trans on Electronic Communications, Vol. 77, Issue 12, pp. 48 – 88, 2016.

20 Sandra Leck, Modern Computer Networks, McGraw-Hill, New York, 2015.

21 Yli-Huumo, J., Ko, D., Choi, S., Park, S., & Smolander, K. (2016). Where is current research on blockchain technology?—a systematic review. PloS one, 11(10), e0163477.

22 R. Stephen and A. Alex, “A Review on BlockChain Security,” IOP Conf. Ser. Mater. Sci. Eng., vol. 396, no. 1, 2018.